REMARKS

Claims 1, 4-18, 20-30, 32-39 remain in this application. Claim 32 has been amended to provide proper antecedent basis. Reconsideration of this application in light of the above amendments and the following remarks is requested.

Objection to Claim 32

Claim 32 has been objected to because it depends on a cancelled claim. By this Response, claim 32 has been amended to depend on claim 24. Accordingly, Applicant respectfully requests the withdrawal of the objection to claim 32.

Rejections Under 35 U.S.C. §103(a), Claims 1, 4, 15, and 16

Claims 1, 4, 15, and 16 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Brothers (U.S. Publication No. 2002/0083178) in view of Schneier (Schneier, Bruce, "Applied Cryptography", Second Edition, 1996, p. 37-39). Applicant traverses this rejection on the grounds that these references are defective in establishing a prima facie case of obviousness with respect to claims 1 and 15.

As the PTO recognizes in MPEP § 2142:

> *... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...*

It is submitted that, in the present case, the examiner has not factually supported a prima facie case of obviousness for the following, mutually exclusive, reasons.

1. Even When Combined, the References Do Not Teach the Claimed Subject Matter

The Brothers and Schneier references cannot be applied to reject claims 1 and 15 under 35 U.S.C. § 103 which provides that:

> *A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that*

the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains ... (Emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. However, neither Brothers nor Schneier discloses "reading contents of the tag including a uniform resource locator of the originator and an encrypted hash", "calculating a second hash from the uniform resource locator of the originator in the tag" and "authenticating the originator of the packet upon determining the decrypted hash and the second hash are identical" as is claimed in claims 1 and 15.

The Examiner alleges that Brothers discloses "reading contents of the tag including URL of the originator and a first hash" in paragraphs 20, 21, 22, and 25. Figure 2D of Brothers is shown below:

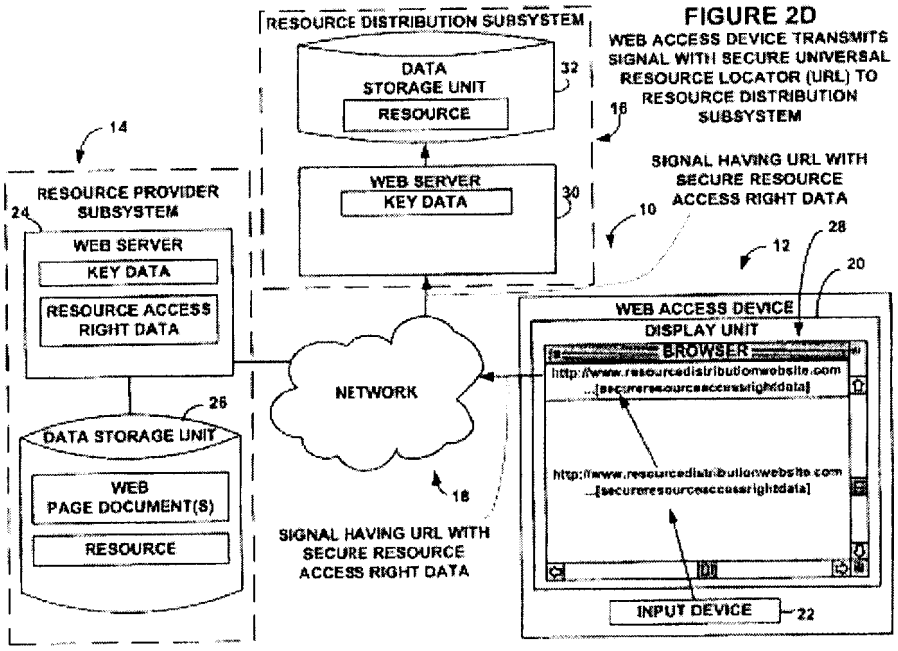


FIGURE 2D
WEB ACCESS DEVICE TRANSMITS SIGNAL WITH SECURE UNIVERSAL RESOURCE LOCATOR (URL) TO RESOURCE DISTRIBUTION SUBSYSTEM

SIGNAL HAVING URL WITH SECURE RESOURCE ACCESS RIGHT DATA

As shown in Figure 2D and in paragraph 93, Brothers discloses that "the Web Access Device 12 generates a signal requesting access to a resource indicated by URL(s) with resource access right data.. . . .WAD 12 transmits the signal requesting access to the resource with the URL(s) with respective secure resource access right data, to web server 30 of the Resource

Distribution System 16." Thus, Brothers merely discloses transmitting a signal to the web server. Brothers does not disclose that the signal is a packet or a tag within the packet. In addition, the URL as disclosed in Brothers is not a URL of the originator of the packet. Instead, the URL belongs to the resource being requested by the Web Access Device. Therefore, Brothers does not disclose "reading the contents of the tag including a uniform resource locator of the originator", as recited in claims 1 and 15.

In addition, Brothers does not disclose "calculating a second hash from the uniform resource location of the originator in the tag." Figure 6 of Brothers is shown below:

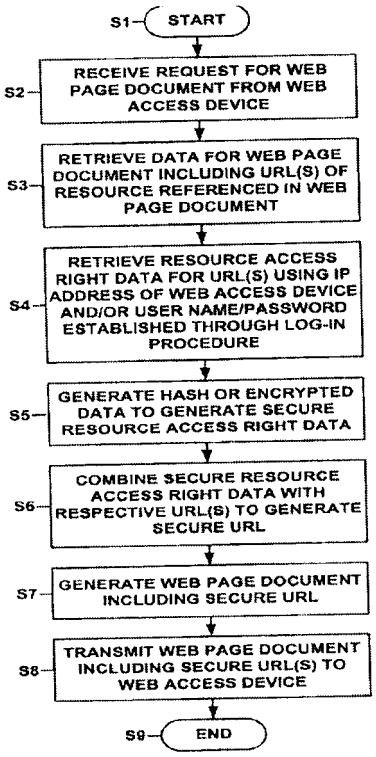


FIGURE 6
PROCESSING PERFORME BY RESOURCE PROVIDEI SUBSYSTEM

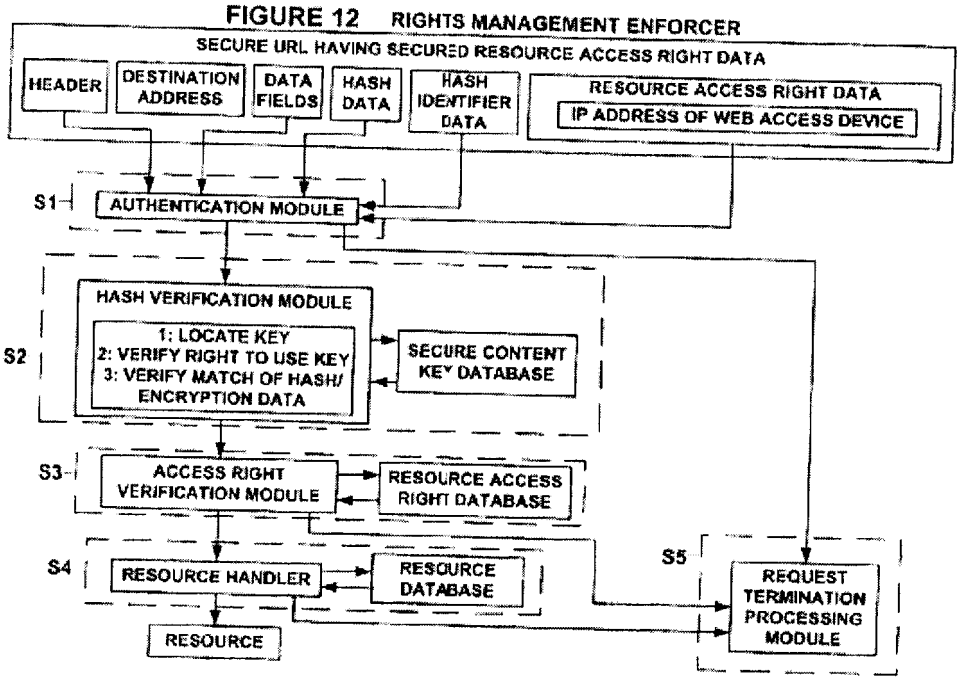
As shown in Figure 6 and in paragraph 105, Brothers discloses:

> In step S3, the processor 42 of the Resource Provider System 14 executes the secure URL generator module to retrieve from its memory 44 data for the requested web page document including URL(s) and data path(s) of the respective resource(s) referenced in the web page document. In step S4 the processor 42 executes the secure URL generator module to retrieve resource access right data for URL(s) using an IP address of the WAD 12 and/or user name and password established by a log-in procedure through execution of the session layer in the ISO/OSI model. In step S5, the processor 42 executes the secure URL generator

> module to retrieve key data from its memory 44. The processor 42 executes such module to generate hash or encrypted data from a portion of the URL, which generally includes the IP address of the WAD 12 and possibly other data as well. The processor 42 further executes the secure URL generator module to combine with the resource access data. In step S6, through execution of the secure URL generator module, the processor 42 combines the secure resource access right data with the URL(s) to produce a secure URL(s), and encodes resulting secure URL into a form readable by the WEAD 12 or server 30 of the RDS 16. In step S7, the processor 42 executes the secure URL generator module to generate a web page document including secure URL(s). In step S8, the processor 42 executes the communication module to transmit the web page document including the secure URL(s) to the WAD 12 via the network 18.

Thus, Brothers discloses generating a hash data from a portion of the URL that includes the IP address of the Web Access Device. The hash data is not generated from the URL of the originator in the tag, but rather the IP address of the Web Access Device. In Figure 10A and in paragraph 158, Brothers discloses that "the unsecured URL, the key data, the IP address of the WAD, and the resource access right data, are combined to form an unsecured URL with unsecured resource access right data. . . .the unsecured URL having resource access right data with appended key data is hashed using a hash generator of the secure URL generator module to generate hash data that includes resource access right data." Thus, Brothers merely discloses generating a hash data using the IP address of the Web Access Device. Nowhere in the reference does Brothers disclose or suggest using the URL of the Web Access Device (originator) to generate hash data. Therefore, Brothers does not disclose "calculating a second hash from the uniform resource location of the originator in the tag", as recited in claims 1 and 15.

Furthermore, Brothers does not disclose "authenticating the originator of the packet upon determining the decrypted hash and the second hash are identical." Figure 12 of Brothers is shown below:



In Figure 12 and paragraph 164, Brothers discloses that "[t]he authentication module receives hash data representing the portion of the resource access right data hashed by the RPS 14. In this example, the hashed data is the result of hashing the IP address. The authentication module also receives the resource access right data including the IP address of the WAD. . . .The authentication module authenticates that the WAD and/or user generated the request to access a resource. For example, the authentication module can perform this function by comparing the IP address within the resource access right data to the IP address included in the header of the HTTP formatted message to ensure that they are the same IP address included."

Brothers merely decodes an IP address of the WAD from the resource access right data (within the secure URL) and compares it with the IP address in the header of the secure URL. Therefore, Brothers compares an extracted IP address with another IP address from the same source. Brothers does not disclose comparing a decrypted hash and a second hash that is calculated from the URL of the originator. In fact, there is no mention of the URL of the originator since Brothers is only concerned with the IP address of the WAD. Therefore, Brothers does not and would not disclose "authenticating the originator of the packet upon determining the decrypted hash and the second hash are identical" as recited in claims 1 and 15.

The Examiner alleges that "it would have been obvious for one of ordinary skill in the art to incorporate the signature techniques of Schneier into the Resource Distribution System in order to prove and verify that the signature is authentic, unforgeable, non-reusable, that the signed document is unalterable, and that the signature cannot be repudiated." Applicants respectfully disagree. Schneier merely discloses encrypting a document with a private key, decrypting the document with a public key, and determining if the decrypted hash matches a generated hash. Similar to Brothers, Schneier does not mention anything about a URL of the originator, let alone calculating a second hash from the uniform resource location of the originator in the tag. Since neither Brothers nor Schneier discloses or suggests calculating a second hash from the URL of the originator in the tag, one of ordinary skill in the art would not have been led to modify or combine the disclosures of Brothers and Schneier to reach the features of claims 1 and 15.

Accordingly, Applicants respectfully submit that neither Brothers nor Schneier discloses or suggests the features of claims 1 and 15 and the rejection of claims 1, 4, 15, and 16 under 35 U.S.C. § 103(a) should be withdrawn.

2. The Combination of References is Improper

There is still another mutually exclusive reason why the Brothers and Schneier references cannot be applied to reject claims 1 and 15 under 35 U.S.C. § 103.

§ 2142 of the MPEP also provides:

> *...the examiner must step backward in time and into the shoes worn by the hypothetical 'person of ordinary skill in the art' when the invention was unknown and just before it was made.....The examiner must put aside knowledge of the applicant's disclosure, refrain from using hindsight, and consider the subject matter claimed 'as a whole'.*

Here, neither Brothers nor Schneier teaches, or even suggests, the desirability of the combination of "reading contents of the tag including a uniform resource locator of the originator and an encrypted hash and calculating a second hash from the uniform resource locator of the originator in the tag," since neither teaches or suggests a URL of the originator. Brothers merely

discloses using the IP address of the WAD to generate a hash data and comparing the IP addresses from the decrypted hash with the IP address of the secure URL. Schneier merely discloses using public and private key for signatures. Neither reference provides any teaching or suggestion of a URL of the originator in a tag or to calculate a second hash using the URL of the originator in the tag.

Thus, it is clear that neither reference provides any incentive or motivation supporting the desirability of the combination. Therefore, there is simply no basis in the art for combining the references to support a 35 U.S.C. § 103 rejection.

In this context, the MPEP further provides at § 2143.01:

> *The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination.*

In the above context, the courts have repeatedly held that obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination.

In the present case it is clear that the examiner's combination arises solely from hindsight based on the invention without any showing, suggestion, incentive or motivation in either reference for the combination as applied to claims 1 and 15. Therefore, for this mutually exclusive reason, the examiner's burden of factually supporting a *prima facie* case of obviousness has clearly not been met, and the rejection under 35 U.S.C. §103 should be withdrawn.

Rejections Under 35 U.S.C. §103(a), Claims 5, 8, 11-14, 17, 18, 20, 23-25, 28-30, 32, and 36-39

Claims 5, 8, 11-14, 17, 18, 20, 23-25, 28-30, 32 and 36-39 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Brothers in view of Schneier and further in view of Blott (EP 1,054,529A2).

With regard to claim 24, Brothers, Schneier, and Blott, either alone or in combination, fail to disclose or suggest "reading contents of the tag including a uniform resource locator of the

originator and an encrypted hash", "calculating a second hash from the uniform resource locator of the originator in the tag" and "authenticating the originator of the packet upon determining the decrypted hash and the second hash are identical". As discussed above, neither Brothers nor Schneier discloses or suggests such features. Blott also does not disclose these features.

In paragraph 39, Blott discloses using a source IP address field and the source port field of the received data packet to associate a service with the received data packet. However, there is no disclosure or suggestion of a URL of the source, let alone calculating a hash from the URL of the source. Therefore, Blott also does not disclose the features of claim 24.

The Examiner alleges that it would have been obvious to incorporate the network usage system of Blott into the resource distribution system of Brothers as modified by Schneier in order to allow the system to monitor and modify a user's quality of service so as to provide appropriate billing for such usage dependent upon the level of quality of service the user receives and/or wishes to get (Paragraph 50). Applicants respectfully disagree.

None of the references discloses or suggests a URL of the originator in a tag and using the URL of the originator to calculate a second hash. Brothers merely discloses using the IP address of the WAD to generate a hash data and comparing the IP address from the decrypted hash with the IP address of the secure URL. Schneier merely discloses using public and private key for signatures. Blott merely discloses associating a service with a source IP address. There is no disclosure or suggestion in any of the references of a URL of the originator in a tag or using the URL of the originator to calculate a second hash. Therefore, one of ordinary skill in the art would not have been led to modify or combine the disclosures of Brothers, Schneier, and Blott to reach the features of claim 24.

Accordingly, Applicants respectfully submit that Brothers, Schneier, and Blott, either alone or in combination, fail to disclose or suggest the features of claims 1, 15, and 24 and the rejection of claims 5, 8, 11-14, 17, 18, 20, 23-25, 28-30, 32 and 36-39 under 35 U.S.C. § 103(a) should be withdrawn.

Conclusion

It is clear from all of the foregoing that independent claims 1, 15, and 24 are in condition for allowance. Dependent claims 4-14, 16-18, 20-23, 25-30, 32-39 depend from and further limit independent claims 1, 15, and 24 and therefore are allowable as well.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

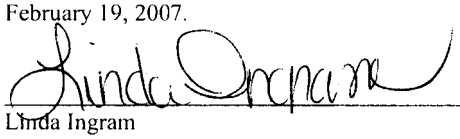
Wing Y Mok
Agent for Applicants
Registration No. 56,237

Dated: February 19, 2007

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8626
Facsimile: 972/692-9075
Client Matter No.: 14686RRUS01U
(22171.386)
R-157478

Certificate of Service

I hereby certify that this correspondence is being filed with the U.S. Patent and Trademark Office via EFS-Web on February 19, 2007.



Linda Ingram